UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,743	12/06/2001	David W. Aucsmith	10559/463001/P10875	2946

20985 7590 05/18/2005

FISH & RICHARDSON, PC
12390 EL CAMINO REAL
SAN DIEGO, CA 92130-2081

EXAMINER	
DERWICH, KRISTIN M	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 05/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/010,743	AUCSMITH ET AL.	
	Examiner	Art Unit	
	Kristin Derwich	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☒ Claim(s) *19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/9/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-38 are pending.

Claim Objections

2. Claim 19 objected to because of the following informalities: the word "many" occurs at line 3, the examiner assumes it should be "may". Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Hereafter patent literature that is referenced as prior art will be cited by column and line number in the form of (column number:line number range). For example, the citation (6:23-27) refers to lines 23-27 of the 6th column in the reference.

3. Claims 1-3, 6-8, 9-11 and 14-34 rejected under 35 U.S.C. 102(e) as being anticipated by Shostack et al. (Shostack), U.S. Patent No. 6,298,445.

As per claim 1:

Shostack discloses a method comprising:

detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem);

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the location (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);

determining at the home location an anomaly based on at least the possible security problem (7:15-16, wherein the security vulnerabilities function as anomalies and the local server is the home location); and

transmitting notice of the anomaly in real time to the client location (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

As per claim 9, this is a computer readable medium version of the claimed method discussed above in claim 1 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 2:

Shostack discloses a method further comprising transmitting notice of the anomaly in real time to other client locations that may communicate with the home location over the network (6:58-59, wherein information about the network status includes anomalies found).

As per claim 10, this is a computer readable medium version of the claimed method discussed above in claim 2 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 3:

Shostack discloses a method further comprising notifying a firewall located between the client location and the home location about the anomaly (4:19-24, wherein the anomaly is an unauthorized user attempting to gain access to the network).

As per claim 11, this is a computer readable medium version of the claimed method discussed above in claim 3 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 6:

Shostack discloses a method in which the anomaly includes unauthorized access to the network (4:64-67; 5:1, wherein this is an example of a security vulnerability (4:47-48) and the security vulnerabilities function as anomalies).

As per claim 14, this is a computer readable medium version of the claimed method discussed above in claim 6 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 7:

Shostack discloses a method in which the anomaly includes unauthorized access of a resource accessible through the network (5:1-4, wherein the program library is a network resource).

As per claim 15, this is a computer readable medium version of the claimed method discussed above in claim 7 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 8:

Shostack discloses a method in which the anomaly includes unauthorized use of resources available through the network (6:10-13, wherein seeing the disk is using a network resource).

As per claim 16, this is a computer readable medium version of the claimed method discussed above in claim 8 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 17:

Shostack discloses a method comprising:

At a home location in a network, receiving from a remote client location an indication of a possible security problem at the client (6:66-67; 7:1, the first application is used to transmit notice of possible security problems and the second application functions to receive information from the first application.) and

determining in real time at the home location an existence of an anomaly based on at least the indication of the possible security problem (7:20-27, wherein the security vulnerabilities function as anomalies).

As per claim 18:

Shostack discloses a method further comprising transmitting notice of the existence of the anomaly in real time from the home location to the remote client

location (7:57-63, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

As per claim 19:

Shostack discloses a method further comprising notice of the existence of the anomaly in real time from the home location to other remote client locations that many communicate with the home location over the network (6:58-59, wherein information about the network status includes anomalies found).

As per claim 20:

The method of claim further comprising notifying, from the home location, a firewall located between the remote client location and the home location about the anomaly.

As per claim 21:

Shostack discloses a method of claim further comprising transmitting information from the home location to the remote client location to help the remote client location identify possible security problems (13:7-9, wherein the database updates to the security vulnerabilities helps to identify possible security problems).

As per claim 22:

Shostack discloses a method further comprising determining the existence of the anomaly based on at least information regarding previous anomalies (9:56-63, wherein the database contains a log of all of the previous security vulnerabilities which function as anomalies).

As per claim 23:

Shostack discloses a method comprising:

detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem);

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the client location (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server); and

receiving in real time at the client location a notice from the home location indicating an existence of an anomaly based on at least the possible security problem (7:57-63; 9:10-21, wherein the client location receives software enhancements which function as the notice of the security vulnerability, which functions as the anomaly).

As per claim 25:

Shostack discloses a method further comprising receiving in real time at the client location a notice from the home location indicating an existence of a possible security problem detected by another client location that can communicate with the home location over the network (6:66-67; 7:1, the first application is used to transmit notice of possible security problems to each computer on the network (6:58-59) and the second application functions to receive information from the first application.).

As per claim 29:

The apparatus of claim 28 in which the first mechanism is also configured to determine the anomaly based on at least information regarding previously determined anomalies.

As per claim 30:

Shostack discloses a system comprising:

a client terminal (9:10);

a server (9:10);

a first client mechanism accessible by the client terminal and configured to detect a possible security problem at the client terminal (6:43-46, wherein an intrusion is a possible security problem);

a second client mechanism accessible by the client terminal and configured to transmit notice of the possible security problem across a network in real time to a server remotely located from the client terminal (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem);

a third client mechanism accessible by the client terminal and configured to receive updates from the server in real time regarding security problems that the first client mechanism may use in detecting possible security problems (7:57-63; 9:10-21, wherein the client receives the software enhancement updates which function as updates from the server about security problems);

a first server mechanism accessible by the server and configured to determine an anomaly based on at least information from a client regarding a possible security problem (7:15-16, wherein the security vulnerabilities function as anomalies and the local server is the home location); and

a second server mechanism accessible by the server and configured to transmit notice of the anomaly in real time over the network to the client terminal (7:57-63; 9:10-

21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

As per claims 26 and 28, combined, these are apparatus versions of the claimed system discussed above in claim 30 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 32:

Shostack discloses a system in which the first server mechanism is also configured to determine the anomaly based on at least information regarding previously determined anomalies (9:56-63, wherein the database contains a log of all of the previous security vulnerabilities which function as anomalies).

As per claim 33:

The system of claim 30 in which the second server mechanism is also configured to transmit notice of the anomaly in real time to other client locations that may communicate with the server over the network (6:58-59, wherein information about the network status includes anomalies found).

As per claim 34:

Shostack discloses a system further comprising a firewall located between the client terminal and the server and configured to act as an intermediary for information flowing between the client terminal and the server (4:19-24, since the server is remotely connected to the network 20 (9:13-14; fig 2, item 20), the placement of the firewall makes it an intermediary between the external server and the client, therefore, the

firewall's functionality as a filter shows that information flows between the server and client).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 4, 12, 24, 27 and 31 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) as applied to claims 1, 9, 23, 26 and 30 above and further in view of Baker, U.S. Patent No. 6,775,657.

As per claim 4:

Shostack fails to teach a method further comprising inspecting a packet that arrives at the client location to detect the possible security problem. However, Baker discloses a method wherein a network based intrusion detection system analyzes network packet data to make security decisions (1:41-42; 46-53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to analyze a packet that arrives at the client in order to make security decisions because this would make the intrusion detection system scale well for network protection since it is the amount of traffic that determines performance, therefore it would also be easier to control and improve performance of the network as a whole (1:53-60).

As per claim 12, this is a computer readable medium version of the claimed method discussed above in claim 4 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 24:

Shostack fails to teach a method further comprising inspecting a packet that arrives at the client location to detect the possible security problem. However, Baker discloses a method wherein a network based intrusion detection system analyzes network packet data to make security decisions (1:41-42; 46-53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to analyze a packet that arrives at the client in order to make security decisions because this would make the intrusion detection system scale well for network protection since it is the amount of traffic that determines performance, therefore it would also be easier to control and improve performance of the network as a whole (1:53-60).

As per claim 27:

Shostack fails to teach an apparatus in which the first mechanism is also configured to monitor packets that arrive at the client terminal for the possible security problem. However, Baker discloses a method wherein a network based intrusion detection system analyzes network packet data to make security decisions (1:41-42; 46-53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to analyze a packet that arrives at the client in order to make security decisions because this would make the intrusion detection system scale well for network protection since it is the amount of traffic that determines performance,

therefore it would also be easier to control and improve performance of the network as a whole (1:53-60).

As per claim 31:

Shostack fails to teach a system in which the first mechanism is also configured to monitor packets that arrive at the client terminal for the possible security problem. However, Baker discloses a method wherein a network based intrusion detection system analyzes network packet data to make security decisions (1:41-42; 46-53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to analyze a packet that arrives at the client in order to make security decisions because this would make the intrusion detection system scale well for network protection since it is the amount of traffic that determines performance, therefore it would also be easier to control and improve performance of the network as a whole (1:53-60).

5. Claims 5, 13 and 35 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) as applied to claims 1, 9 and 30 above and further in view of Bowman-Amuah, U.S. Patent No. 6,697,824.

As per claim 5:

Shostack fails to teach a method in which the network includes a virtual private network. However, Bowman-Amuah discloses a method wherein a network is protected from unauthorized access through the encryption services provided by Virtual Private Networking (75:64-65, fig 36). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a virtual private network with the

network because of the added security benefits a VPN affords a system against unauthorized users.

As per claim 13, this is a computer readable medium version of the claimed method discussed above in claim 5 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 35:

Shostack fails to teach a system in which the firewall includes a corporate server. However, Bowman-Amuah discloses a method wherein a corporate firewall includes a corporate server at a corporate headquarters (75:65-66; 76:19-23). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a corporate server with the firewall because if the intrusion detection system were to be used in a business setting the firewalls would provide increased access control for the internal network (76:21-23).

6. Claims 36-38 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) in view of Bowman-Amuah (U.S. 6,697,824).

As per claim 36:

Shostack substantially teaches a method comprising:

processing information relating to possible security problems at a home location to determine a security problem (7:52-54, wherein the updating of the database functions as processing information relating to security problems and this database is used to help determine a security problem); and

modifying a monitoring agent that is included at each one of multiple clients to reflect the security problem, each one of the multiple clients capable of communicating the information to the home location (9:32-37, wherein the software enhancements modify the monitoring agent to reflect the security problem and since it can interrogate the server, this functions as communicating with the home location).

Shostack fails to teach a method associated with a private network. However, Bowman-Amuah discloses a method wherein a network is protected from unauthorized access through the encryption services provided by Virtual Private Networking (75:64-65, fig 36). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a virtual private network with the network because of the added security benefits a VPN affords a system against unauthorized users.

As per claim 37:

Shostack and Bowman-Amuah substantially teach a method as applied to claim 36 above and furthermore, Shostack discloses a method further comprising performing the modifying in real time (7:33-35).

As per claim 38:

Shostack and Bowman-Amuah substantially teach a method as applied to claim 36 above and furthermore, Shostack discloses a method in which the multiple clients can communicate the information in real time (6:53-54; 58-59).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kristin Derwich
Examiner
Art Unit 2132

KD

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100